UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,177	05/15/2006	Joachim Hagmeier	DE920030011US1	7861

25259 7590 10/17/2008

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
10/17/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

RSWIPLAW@us.ibm.com

Office Action Summary	Application No.	Applicant(s)	
	10/564,177	HAGMEIER ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20060110*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-20 are pending.

Claim Objections

1. Claims 1-20 are objected to because of the following informalities:

   - The claims refer to a "header request", which is never discussed in the specification. The specification refers to a "request header", however, and this is how the "header request" of the claims has been construed. The application never requests a header, but rather provides authentication information in the header of a request. Therefore, for purposes of prior art rejection, “header request” has been construed as “request header” every time it is mentioned.
   - Claim 1 recites inserting client authentication information into a request header “independently of the authentication process used by said server”, which does not make sense. As seen by the final limitation of claim 1, for example, authentication is performed on the server without any additional information being sent, so it appears as though the authentication information must be used in an authentication process of the server. For purposes of prior art rejection, this has been construed as being an extension of the server not requesting such authentication information, but will need to be clarified in the response.

   Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 4, 5, 8, 11-17, 19, and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The following is an exemplary list of the antecedent basis issues in the claims. Claim 1 recites “the header request”, “the authentication process”, and "said server" before any of those limitations have been set forth in the claim. Claim 4 recites "the client certificate", which has insufficient antecedent basis as well. Claim 14 recites “said authentication component”, “said public key”, “the client certificate”, “said digital signature”, “the HTTP-request header”, and “the same hash algorithm”, none of which have antecedent basis. Claim 17 recites “the client certificate”, “the hash value” and “Client’s private key”, none of which have antecedent basis. The above is non-exhaustive and other claims have like antecedent basis issues.

Claim Rejections - 35 USC § 101

3. Claims 15-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 16, for example, refers to a client system comprising “a browser” and “a component for inserting client authentication information”, both of which appear as though they could be purely software. A browser

Is known in the art to be software, and paragraphs 26-29 of the current specification discuss insertion and signature components being purely software. The components of independent claims 15 and 19 also appear as though they could be purely software. Since claims 15-19 are directed to systems of software, per se, they are non-statutory. In order to be statutory, the claims must recite as a limitation a physical component (e.g., a processor, assuming the specification has basis for a processor being a physical component).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-5, 8-9, 11-17, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maurin (U.S. Patent Application Publication 2002/0133700) in view of Buch (U.S. Patent Application Publication 2003/0217165).

Regarding Claim 1,

Maurin discloses a method for authenticating clients in a client-server environment, wherein the client-server environment uses a communication protocol that allows extensions of a request header without violating the communication protocol, wherein the method comprises the steps of:

Generating a request header (Paragraphs 18-19);

Inserting client authentication information into the request header resulting in an extended request header independently of an authentication process used by a server (Paragraphs 18-25); and

Sending the extended request header to a server (Paragraphs 18-25);

But does not explicitly disclose receiving information from the server if authentication has been successful or that the insertion is performed without the server requesting authentication information (though Maurin does appear as though it works this way).

Buch, however, discloses inserting client authentication information into a request header without the server requesting authentication information, sending the extended header to a server, and receiving information from the server if authentication has been successful (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that

certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Regarding Claim 20,

Claim 20 is a computer program product claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Maurin as modified by Buch discloses the method of claim 1, in addition, Maurin discloses that the communication protocol is HTTP (Paragraphs 18-25).

Regarding Claim 3,

Maurin as modified by Buch discloses the method of claim 1, in addition, Buch discloses that the authentication information is included in the first request header for establishing a session with the server (Figures 6-7; and Paragraphs 53-54).

Regarding Claim 4,

Maurin as modified by Buch discloses the method of claim 1, in addition, Maurin discloses that the authentication information comprises a client certificate containing a client name and a client public key (Paragraph 28); and Buch discloses that the authentication information comprises a client certificate containing a client name and a client public key, and a digital signature which has been generated over a hash value

of the request header including the client certificate using a client private key (Figures 6-7; and Paragraphs 26-27, 39, 44, and 53-54).

Regarding Claim 5,

Maurin as modified by Buch discloses the method of claim 1, in addition, Maurin discloses that the authentication information is automatically inserted into the request header by a browser on the client (Paragraphs 24-26).

Regarding Claim 8,

Maurin discloses a method for authenticating clients in a client-server environment, wherein the client-server environment uses a communication protocol that allows extensions of a request header without violating the communication protocol, wherein a system establishes communication between a client and a server, wherein the method comprises the steps of:

Receiving a request header from the client (Paragraph 32);

Inserting authentication information into the request header resulting in an extended request header independently of an authentication process used by the server (Paragraphs 49-54);

Sending the extended request header to a server (Paragraphs 49-54); and

But does not explicitly disclose receiving information from the server if authentication has been successful or that the insertion is

performed without the server requesting authentication information (though Maurin does appear as though it works this way).

Buch, however, discloses inserting client authentication information into a request header without the server requesting authentication information, sending the extended header to a server, and receiving information from the server if authentication has been successful (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Regarding Claim 9,

Maurin as modified by Buch discloses the method of claim 8, in addition, Maurin discloses that the system can be a proxy server, a gateway, or a tunnel (Paragraph 13).

Regarding Claim 11,

Maurin as modified by Buch discloses the method of claim 8, in addition, Maurin discloses that the authentication information comprises a

client certificate containing a client name and a client public key (Paragraph 28); and Buch discloses that the authentication information comprises a client certificate containing a client name and a client public key, and a digital signature which has been generated over the whole request header including the client certificate using a client private key (Figures 6-7; and Paragraphs 26-27, 39, 44, and 53-54).

Regarding Claim 12,

Maurin discloses a method for authenticating clients in a client-server environment, wherein the client-server environment uses a communication protocol that allows extensions of a request header without violating the communication protocol, wherein at a server side the method comprises the steps of:

Receiving a client request header containing authentication information (Paragraphs 18-25);

Validating the authentication information contained in the request header by a server authentication component (Paragraphs 5 and 28); and

But does not explicitly disclose providing information to a client if authentication has been successful

Buch, however, discloses validating authentication information received in a request header and providing information to a client if authentication has been successful (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Regarding Claim 13,

Maurin as modified by Buch discloses the method of claim 12, in addition, Maurin discloses that the authentication information comprises a client certificate containing a client name and a client public key (Paragraph 28); and Buch discloses that the authentication information comprises a client certificate containing a client name and a client public key, and a digital signature which has been generated over the whole request header including the client certificate using a client private key (Figures 6-7; and Paragraphs 26-27, 39, 44, and 53-54).

Regarding Claim 14,

Maurin as modified by Buch discloses the method of claim 12, in addition, Maurin discloses that the communication protocol is HTTP and that the request header is an HTTP-request header (Paragraphs 18-25)

and Buch discloses that the server authentication component performs the steps of:

Accessing a public key contained in a client certificate (Paragraphs 26-28);

Decrypting a digital signature contained in a request header with the public key resulting in a hash value (Paragraph 28);

Applying a hash algorithm that was used by the client to the request header (Paragraph 28); and

Considering authentication as successful if both hash values match (Paragraph 28).

Regarding Claim 15,

Maurin discloses a server system for authentication clients in a client-server environment, wherein the client-server environment uses a communication protocol that allows extensions of a request header without violating the communication protocol, wherein a client provides authentication information in the request header to a server system, wherein the server system comprises:

An authentication component with the functionality to read the authentication information contained in an incoming client request header, and to validate the authentication information (Paragraphs 5 and 18-28);

But does not explicitly disclose the server requesting authentication information (though Maurin does appear as though it works this way).

Buch, however, discloses that the client request header was sent with authentication information contained therein without the server having requested the authentication information from the client (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Regarding Claim 16,

Maurin discloses a client system to be authenticated by a server system in a client-server environment, wherein the client-server environment uses a communication protocol that allows extensions of a request header without violating the communication protocol, wherein the client system comprises:

A browser (Paragraphs 24-26); and

A component for inserting client authentication information into the request header independently of an authentication process used by the server (Paragraphs 18-25);

But does not explicitly disclose insertion is performed without the server requesting authentication information (though Maurin does appear as though it works this way).

Buch, however, discloses inserting client authentication information into a request header without the server requesting authentication information (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Regarding Claim 17,

Maurin as modified by Buch discloses the system of claim 16, in addition, Maurin discloses that the authentication information comprises a client certificate containing a client name and a client public key (Paragraph 28); and Buch discloses that the authentication information comprises a client certificate containing a client name and a client public key, and a digital signature which has been generated over a hash value

of the request header including the client certificate using a client private key (Figures 6-7; and Paragraphs 26-27, 39, 44, and 53-54).

5. Claims 6-7 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maurin in view of Buch, further in view of Bishop (U.S. Patent 7,343,351).

Regarding Claim 6,

Maurin as modified by Buch does not explicitly disclose that the client's browser receives the authentication information from a smart card via a smart card reader.

Bishop, however, discloses that the client's browser receives the authentication information from a smart card via a smart card reader (Column 17, lines 27-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card of Bishop into the authentication system of Maurin as modified by Buch in order to provide a smart card that is dedicated to security procedures in order to sign data and create authentication information, thereby increasing security by making it more difficult for a malicious entity to steal data from such a secure smart card.

Regarding Claim 7,

Maurin as modified by Buch discloses the method of claim 1, in addition, Maurin discloses that the authentication information is automatically inserted into the request header (Paragraphs 24-26); but

does not explicitly disclose that the authentication information is received from a smart card via a smart card reader.

Bishop, however, discloses that the authentication information is received from a smart card via a smart card reader (Column 17, lines 27-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card of Bishop into the authentication system of Maurin as modified by Buch in order to provide a smart card that is dedicated to security procedures in order to sign data and create authentication information, thereby increasing security by making it more difficult for a malicious entity to steal data from such a secure smart card.

Regarding Claim 18,

Maurin as modified by Buch does not explicitly disclose a smart card reader; and a smart card with a security module containing the client private key and a client certificate containing client name and private key, wherein the smart card provides the certificate together with a digital signature to the inserting component, wherein the digital signature is the result of an encryption of a hash value of the request header containing the certificate information by means of the private key.

Bishop, however, discloses a smart card reader; and a smart card with a security module containing the client private key and a client certificate containing client name and private key, wherein the smart card

provides the certificate together with a digital signature to the inserting component, wherein the digital signature is the result of an encryption of a hash value of the request header containing the certificate information by means of the private key (Column 17, lines 27-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card of Bishop into the authentication system of Maurin as modified by Buch in order to provide a smart card that is dedicated to security procedures in order to sign data and create authentication information, thereby increasing security by making it more difficult for a malicious entity to steal data from such a secure smart card.

6. Claims 10 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maurin in view of Buch, further in view of Rhodes (U.S. Patent Application Publication 2002/0049902)

Regarding Claim 10,

Maurin as modified by Buch discloses the method of claim 8, in addition, Maurin discloses that the communication protocol is HTTP and the authentication information is automatically inserted into an HTTP-request header by an insertion component (Paragraphs 18-25); but does not explicitly disclose that the authentication information is received from a signature component.

Rhodes, however, discloses that the authentication information is received from a signature component (Figure 7; and Paragraphs 75-77). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the intelligent network element of Rhodes into the authentication system of Maurin as modified by Buch in order to allow authentication and encryption to ensue even in the event that the client is unable to perform such functionality, by allowing an intelligent network element to proxy such services, thereby ensuring that communication across insecure networks is secured even when the client cannot authenticate itself or encrypt data.

Regarding Claim 19,

Maurin discloses a proxy server system for providing client authentication information to a server system, wherein the proxy server system has a communication connection with a client system and a server system, wherein a communication protocol used between the systems allows extensions of a request header without violating the communication protocol, wherein the proxy server system comprises:

A proxy insertion component for inserting a client certificate into the request header received from the client independently of an authentication process used by the server (Paragraphs 18-25);

But does not explicitly disclose that the insertion is performed without the server requesting authentication information (though Maurin

does appear as though it works this way), or a signature component for creating a digital signature and providing it together with the client certificate to the proxy insertion component.

Buch, however, discloses inserting a client certificate and a digital signature into the request header without the server requesting authentication information (Figures 6-7; and Paragraphs 26-27, 39, 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Rhodes, however, discloses a signature component for creating a digital signature and providing it together with the client certificate to the proxy insertion component (Figure 7; and Paragraphs 75-77). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the intelligent network element of Rhodes into the authentication system of Maurin as modified by Buch in order to allow authentication and encryption to ensue even in the event

that the client is unable to perform such functionality, by allowing an intelligent network element to proxy such services, thereby ensuring that communication across insecure networks is secured even when the client cannot authenticate itself or encrypt data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437